REMARKS

The Office Action dated June 13, 2007 has been received and carefully noted. The following remarks, are submitted as a full and complete response thereto.

The Applicants wish to thank the Examiner for indicating allowable subject matter in claims 2-14, 21 25-36, 38, and 45. In view of the Response to a Restriction Requirement filed on March 16, 2007, claims 16-20 and 40-44 are withdrawn from consideration.

As will be discussed below, it is also requested that all of claims 13, 22, 23, 37, 46, and 47 be found allowable as reciting patentable subject matter.

Claims 2-14, 22-23, 25-38, and 45-47 are pending and under consideration.

REJECTION UNDER 35 U.S.C. § 103:

At page 2 of the Office Action, claims 13, 22, 23, 37, 46, and 47 was rejected under 35 U.S.C. § 103(a) as being unpatentable over EP 1191763 to McCann et al. ("McCann") in view of U.S. Patent No. 6,144,431 to Matsumoto et al. ("Matsumoto"). The Office Action took the position that McCann describes all the recitations of independent claims 13, 22, 23, 37, 46, and 47. Applicants respectfully traverse this rejection.

Independent claim 13 recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile

communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, and if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login.

Independent claim 22 recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a user identification to the subscriber terminal corresponding to the mobile subscriber identification data and using the transmitted user identification in connection with login.

Independent claim 23 recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a user identification to the data transfer device over a data transfer connection and using the transmitted user identification in connection with login.

Independent claim 37 recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to

- 23 -

the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a second password from the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to also use the second password in connection with login.

Independent claim 38, upon which claims 25-36 and 45 are dependent, recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile

communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a confirmation identifier via the service access point to the data transfer device over the first data transfer connection and to transmit the same confirmation identifier to the subscriber terminal together with the password.

Independent claim 46 recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a

user identification to the subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login to the service access point.

Independent claim 47 recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit the user identification via the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to use the user

identification transmitted to the data transfer device in connection with login to the service access point.

As will be discussed below, McCann and Matsumoto fail to disclose or suggest the elements of any of the presently pending claims.

McCann generally describes an authentication system in which a user requesting visiting access to the W-LAN is required to have a valid cellular mobile account, a portable computing device with a browser and a valid W-LAN card from another operator that administers a home authentication, authorization, and accounting (HAAA) server. The user inputs identity information that enables the HAAA to issue a personal identification number (PIN) which is encoded and forwarded to the user's mobile telephone. The encoded PIN is transferred to the browser to authenticate the requested visiting access to the W-LAN.

Matsumoto generally describes in FIG. 14, a radio communication exchange system A and a radio communication exchange system B connected to a public key management device 100. See column 18, lines 20-47. A personal station PS1 has PSN1 as PSN of PS1 and a private key Ks1 stored therein. Further, when PS1 moves to the radio communication exchange system, a key k1 or k1' peculiar to each radio communication exchange system is stored into PS1 at the same memory position.

However, McCann fails to teach or suggest, "if a valid access right exists, generating a password, transmitting the **password** to a subscriber terminal **corresponding to the mobile subscriber identification data,** and logging in to the

- 27 -

service access point from the data transfer device using the password transmitted to the subscriber terminal," emphasis added, as recited in independent claim 13. In paragraphs [0013], [0014], and [0026] of McCann there is not teaching or suggestion providing that a user ID is transmitted to the subscriber terminal as in the present invention. Instead, McCann discloses in those paragraphs that a PIN encoded with a registration number is transmitted to a handset of a mobile user. The registration number is public, and cannot be considered as a user ID that is user specific (See paragraphs [0022] and [0023] of McCann).

In addition, paragraph [0017] of McCann describes that the home AAA 8 generates a PIN, which is then encoded with the original masking data string and passed to a local short message service centre (SMSC) 9. However, McCann does not teach or suggest that the SMSC 9 corresponds to the mobile subscriber identification data. Rather, McCann simply describes that a PIN is generated and transmitted to the SMSC 9. McCann does not describe that the SMSC 9 corresponding to the identification data of the subscriber of the mobile communications system. Thus, McCann fails to teach or suggest, at least, "if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal," as recited in independent claim 13.

Furthermore, as correctly recognized in the Office Action, McCann fails to teach or suggest, "transmitting a second password from the service access point to the data

transfer device over a data transfer connection, the second password being also used in connection with login," as recited in independent claim 13. Accordingly, the Office Action relied on Matsumoto as curing the deficiencies of McCann.

However, contrary to the contentions made in the Office Action, Matsumoto does not teach or suggest a transmission of a second password, which is also used in **connection with the login** as the first password, from a service access point to a data transfer device as in the present claims. Rather, in FIG. 14 of Matsumoto, when PSI moves to a service area of the radio communication exchange system A formed by an exchange 103-a, the exchange 103-a fetches a public key Ko1 of PS1 from the public key management device 100 and registers it into a key DB 111-a to perform the authentication of PS1. See column 18, lines 33-47. **After a success in authentication, the exchange 103-a of Matsumoto generates k1** as a peculiar authentication key of PS1, registers k1 into the key DB 111-a, and informs PS1 of k1. (Emphasis added) From that time onward, PS1 holds the peculiar authentication key k1 stored in the station information table 1000, so far as PS1 does not move to the outside of the service area of the exchange 103-a. Even assuming that k1 is considered to be a second password (not admitted), k1 of Matsumoto is not generated in connection with a login. Matsumoto clearly describes that k1 is generated after a successful authentication.

Rather, the peculiar authentication key k1 of Matsumoto is used for further authentication within a service area of a specific communication exchange system (after an initial authentication with a public key k1 fetched from a public key management

device). Applicants respectfully assert that k1 cannot correspond with the second password or the user identification to be used in an initial login, as k1 is used for subsequent authentication and not together with the original authentication key in the first authentication. Therefore, k1 cannot be the second key of independent claim 13 (and independent claim 37) and it is even more clear that it is not a user identification of any sort of independent claims 22 and 23 (and independent claims 46 and 47).

Independent claim 22 recites, in part, "transmitting a user identification to the subscriber terminal corresponding to the mobile subscriber identification data and using the transmitted user identification in connection with login," independent claim 23 recites, in part, "transmitting a user identification to the data transfer device over a data transfer connection and using the transmitted user identification in connection with login," independent claim 37 recites, in part, "the authentication server is configured to transmit a second password from the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to also use the second password in connection with login," independent claim 46 recites, in part, "the authentication server is configured to transmit a user identification to the subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login to the service access point," and independent claim 47 recites, in part, "the authentication server is configured to transmit the user identification via the service access point to the data

transfer device over the first data transfer connection and the data transfer device is configured to use the user identification transmitted to the data transfer device in connection with login to the service access point." Because independent claims 22, 23, 37, 46, and 47 include similar claim features as those recited in independent claim 13, although of different scope, and because the Office Action refers to similar portions of the cited references to reject independent claims 22, 23, 37, 46, and 47, the arguments presented above supporting the patentability of independent claim 13 are incorporated herein to support the patentability of independent claims 22, 23, 37, 46, and 47.

Therefore, a combination of McCann and Matsumoto would fail to teach or suggest all the recitations of independent claims 13, 22, 23, 37, 46, and 47.

Accordingly, in view of the foregoing, it is respectfully requested that independent claims 13, 22, 23, 37, 46, and 47 be allowed.
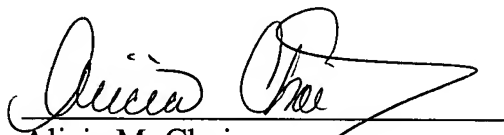

CONCLUSION:

In view of the above, Applicant respectfully submits that the claimed invention recites subject matter which is neither disclosed nor suggested in the cited prior art. Applicant further submits that the subject matter is more than sufficient to render the claimed invention unobvious to a person of skill in the art. Applicant therefore respectfully requests that each of claims 13, 22, 23, 37, 46, 47 be found allowable, along with allowed claims 2-14, 21 25-36, 38, and 45, and this application pass to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicant respectfully petitions for an appropriate extension of time.

Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

<div style="text-align:right">

Respectfully submitted,

Alicia M. Choi
Registration No. 46,621

</div>

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

AMC:dc

Enclosures: